INSTRUMENT MISSION ASSURANCE AND SAFETY REQUIREMENTS FOR THE OUTER PLANETS PROGRAM

August 1999

INSTRUMENT MISSION ASSURANCE AND SAFETY REQUIREMENTS

Table of Contents

INSTRUMENT MISSION ASSURANCE AND SAFETY REQUIREMENTS

1. System Contractors

All contractors and sub-contractors shall meet the requirements of this document unless an approved waiver has been signed by the OP/SP Science Instrument Payload Manager.

2. Parts Requirements

The JPL Parts Program Manager or Mission Assurance Manager shall approve all contractor submitted Parts Plans.

2.1 Parts Quality

All packaged parts shall, as a minimum, meet the Class B (or QML [Qualified Manufacturer Listing] Q) requirements specified in the appropriate MIL standard. Class S parts shall be used where appropriate. Lot Destructive Physical Analyses (DPAs) are required.

All bare die shall be screened and electrically qualified to Class B (QML Q) requirements with JPL approval. Wafer scanning electron microscope inspection is required.

2.2 Radiation Tolerance

2.2.1 Total Ionizing Dose (TID)

All parts shall operate within post-irradiation specification following exposure to the TID level for their applicable mission. A radiation design margin (RDM) of 1.5 for Europa and 2 for Pluto and Solar Probe is recommended for each active semiconductor component. The RDM is applied by dividing the part’s tolerance to TID by the RDM. The resulting TID value is then used to determine the appropriate amount of shielding required as shown in the dose vs. depth curve for the mission. The referenced environments are indicated in the dose vs. depth curves of the OP/SP Environmental Requirements, which can be found in the Outer Planets Program Library at Internet URL http://outerplanets.LaRC.NASA.gov/outerplanets.

All Bipolar and BiCMOS parts shall be evaluated for susceptibility to low-dose-rate effects. Due to lot-to-lot variations of non-hardened components, it is required to perform radiation lot acceptance tests (RLAT).

2.2.2 Displacement Damage

All parts shall be evaluated for susceptibility to displacement damage effects.

2.2.3 Single Event Latchup (SEL)

All parts shall exhibit no latchup to an effective Linear Energy Transfer (LET) = 75 $MeV/mg/cm^2$.

2.2.4 Single Event Upset (SEU)

All parts shall satisfy any of the following three requirements:

1. No upsets to an LET = 75 $MeV/mg/cm^2$ or greater, OR
2. Verification of a device bit error rate of 10^{-10} per day, OR
3. Must meet the requirements for the overall subsystem upset rate requirement.

2.2.5 Single Event Burnout (SEB)

All power transistors operated in the off-mode shall be evaluated for SEB at the lowest application voltage (V_{BE}, V_{GS}). The established survival voltage (V_{CE} for bipolar and V_{DS} for MOSFETs) shall be established from exposure to an ion with a minimum LET of 26 $MeV/mg/cm^2$ and with a range greater than 35 microns. The application voltage shall be derated to 75% of the established survival voltage. All testing shall be performed with normal beam incidence and at ambient (room) temperature.

- Drain voltage rating ≤ 100 V — Ion range 25 μm or more
- Drain voltage rating between 100 and 250 V — Ion range 40 μm or more
- Drain voltage rating above 250 V — Ion range 80 μm or more

2.2.6 Single Event Gate Rupture (SEGR)

All power MOSFETs operated in the off-mode may be susceptible to, and shall be evaluated for, single event gate rupture (SEGR) at the lowest application V_{GS}. The established survival voltage (V_{DS}) shall be established from exposure to an ion with a minimum LET of 26 $MeV/mg/cm^2$ and with a range greater than 35 microns. The application voltage shall be derated to 75% of the established survival voltage. All testing shall be performed at normal beam incidence and at ambient room temperature.

- Drain voltage rating ≤ 100 V Ion range 25 μm or more
- Drain voltage rating between 100 and 250 V Ion range 40 μm or more
- Drain voltage rating above 250 V Ion range 80 μm or more

2.3 Parts Acquisition

2.3.1 Heritage parts

Residual inventory (i.e., heritage parts), in this context, refers to parts previously approved and procured for prior flight Project applications. Residual electronic parts may be used for OP/SP Science Instruments only if they meet all requirements of this document.

2.3.2 Parts Procurement

Purchase orders shall not take exception to reference specifications or requirements therein unless approved by the OP/SP Science Instrument Parts Program Manager or via waiver.

2.3.3 Customer Source Inspection

Pre-seal visual inspection shall be performed on all packaged, flight ASICs, hybrid microcircuits, and nonstandard relays by JPL.

2.3.4 Radiation Lot Acceptance Testing (RLAT)

Device types that are shown to be marginal by a TID characterization test or analysis and are still requested for use in flight equipment shall be subject to RLAT.

2.3.5 Destructive Physical Analysis (DPA)

Grade-2/Class-B packaged electronic parts require DPA. DPAs shall be performed on a sample of each manufacturing lot date code for crystals, filters, ceramic capacitors (except MIL-C-123), relays, MIL-C-39010 inductors, and all nonstandard packaged parts (including multi-chip modules and hybrids). MIL-C-39010 inductors/transformers shall be sectioned to examine the adequacy of the termination. Relays shall have an internal visual examination. Chip capacitors and resistor networks require a DPA.

The results of the DPA shall be evaluated by the procuring activity, and the lot shall be accepted or rejected based on the criteria of the specification.

2.4 Electronic Parts Application

2.4.1 Parts Derating

Each part used in flight equipment shall be applied in a manner such that the temperatures experienced and electrical stresses produced when it is operating do not exceed the derating criteria defined in JPL D-8545 "Electronic Parts Section Derating Guidelines."

2.4.2 Electrostatic Discharge (ESD) Control

ESD damage or degradation may occur in static-sensitive electronic parts during handling of the parts from procurement through incoming inspection, testing, screening, storing and final assembly/test. To protect static-sensitive parts from ESD, handling of parts shall be controlled by the requirements of JPL D-1348 "Electrostatic Control for Assembly and Test Area for Flight Projects."

2.4.3 NASA and Government Industry Data Exchange Program (GIDEP) Alerts

All hardware-delivering design agencies, both internal and external to JPL, are responsible for reviewing all Alerts, and for immediately reporting corrective action for applicable Alerts (i.e. for parts used in the hardware) to the project.

The design agency shall present a report at the CDR, and another at the Pre-Ship Review, that lists all of the Alerts that are pertinent to the parts used in the flight design, the possible impact should the part fail, and the actions proposed and those taken. It is the responsibility of the design agency to avoid the use of defective parts in flight equipment.

2.4.4 Parts Failure Analysis

Failure analysis is required for all part failures that occur subsequent to screening. The only exceptions are parts damaged by human error (e.g., improper installation). Analysis shall be carried to the point that lot dependency of the failure mode can be determined. Failure analysis reports shall be written to document the analysis approach, the determined failure mode and mechanism (i.e., cause) responsible for the failure, and the corrective actions required to prevent recurrence of the failure. If a lot dependency is found, the JPL Mission Assurance Manager (MAM) will disposition the slices using the suspect lot.

2.4.5 As-Built Parts List

An As-Built Parts List shall be released prior to hardware integration and test. In addition to the information required in the Preliminary Parts Lists, the As-Built Parts List shall include for each different part the actual part marking, part number purchased, manufacturer, lot date code, serial number (for serialized parts), wafer and wafer lot numbers (when required), parts test lot numbers (where applicable), procurement specification number, traceability number (when assigned by the cognizant parts organization), the serial number and part number of the next assembly level into which the part is installed (e.g., board or module), and the reference designator of the location where each part is used on the next assembly level. The as-built parts list shall be supplied to the JPL Electronic Parts Engineering Section in a computer-readable format.

3. Reliability Assurance

3.1 Analysis Requirements

Parts stress analysis shall be required on all electronic circuits in accordance with the derating requirements of JPL D-8545.

Worst Case Analysis (WCA) is required.

Failure Modes, Effects and Criticality Analysis (FMECA) is required at all slice and assembly level interfaces including support equipment (SE) interfaces.

Circuit designs containing Single Event Effects (SEE) sensitive parts shall be analyzed to identify the effect of SEEs and to assure compliance with requirements. The requirements regarding performance with respect to SEE during operation for any microprocessor or its peripheral family, or any other parts, are as follows:

a. Temporary loss of function or loss of data shall be permitted provided that the loss does not compromise subsystem/system health, full performance can be recovered rapidly, and there is no time in the mission that the loss is mission critical.

b. Normal operation and function shall be restored via internal correction methods without external intervention in the event of an SEU.

c. Fault traceability shall be provided in the telemetry stream to the greatest extent practical for all anomalies involving SEEs.

3.2 Single Failure Points

All single failure points (SFP) shall be identified. Success critical SFP's shall be indicated. No safety critical SFP's are allowed.

3.3 Operating Time

All instrument electronics shall be operated for a minimum of 500 hours as the requirement and total of 1000 hours as a goal prior to launch.

4. Problem Failure Reporting (PFR)

4.1 Problem Log and PFR Starting Points

Problem Log for:

(1) Hardware to begin at first application of power of each Engineering Model (EM) or Protoflight assembly.
(2) Software to begin at S/W development integration and test.
(3) Ground Support Equipment (GSE) hardware and software (including test and facility equipment) during GSE acceptance testing.

PFRs for:

(1) Hardware and Software to begin at system level integration and test.
(2) Support equipment hardware and software (including test and facility equipment) while testing the items listed in (1) above.

4.2 Criticality and Cause/Corrective Action Rating

Each PFR shall be assigned a two-factored rating. Problem Logs require the cause/corrective action rating only.

Failure Effect Ratings:

a. Rating 1: Negligible effect on mission performance and system safety.

(1) No appreciable change in functional capability.
(2) Minor degradation of engineering or science capability.
(3) Support equipment or test equipment problem/failure.
(4) SE, TE, or operator induced failure.
(5) Workmanship failures found at initial test opportunity.
(6) Causes negligible operational difficulties or constraints.
(7) Negligible or no reduction in lifetime.
(8) Cannot occur in flight.

b. Rating 2: Significant effect on mission performance or system safety.

(1) Appreciable change/degradation in functional capability.
(2) Appreciable degradation of engineering or science capability.
(3) Causes significant operational difficulties or constraints.
(4) Significant reduction in lifetime.

c. Rating 3: Major or catastrophic effect on mission performance or system safety.

(1) Major change/degradation in functional capability.
(2) Major degradation of engineering or science capability.
(3) Causes major operational difficulties or constraints.
(4) Major reduction in lifetime.

Cause and Corrective Action Ratings:

a. Rating 1: Known Cause/Certainty in corrective action.

Analysis, corrective action, and verification of correction are considered to have determined the cause and have defined an effective corrective action that has been implemented and verified by test or other demonstration. No known possibility of recurrence in flight.

b. Rating 2: Unknown Cause/Certainty in corrective action.

The cause could not be completely determined, but an effective corrective action has been implemented and verified by test or other demonstration; or the problem/failure (observed incident) could not be repeated in tests or checkouts. No known possibility of recurrence in flight.

c. Rating 3: Known Cause/Uncertainty in corrective action.

Analysis, corrective action and verification of correction are considered to have determined the cause, but effective corrective action has not been implemented and verified by test or other demonstration. Some possibility exists of recurrence in flight.

d. Rating 4: Unknown Cause/Uncertainty in corrective action.

The cause could not be completely determined and no effective corrective action has been implemented and verified by test or other demonstration. Some possibility exists of recurrence in flight.

4.3 Red Flag Problem Logs and PFR's

All PFR's having a failure effect rating of 2 or 3 coupled with a failure cause/ corrective action rating of 3 or 4 are defined as "Red Flag" PFR's.

a. Each Red Flag PFR must include a statement regarding the rationale for accepting the residual risk.

b. The JPL Science Instrument Payload Manager and the Contractor Program Manager (if applicable) shall review, approve, and sign Red Flag PFR closures to acknowledge understanding and acceptance of the defined residual mission risk.

c. All Red Flag PFRs shall be discussed at subsequent formal reviews.

4.4 Safety Rating and Assessment

All Problem Logs and PFRs with a hardware or personnel safety issue shall have a safety risk assessment made by the JPL Systems Safety office and shall be signed by the JPL Systems Safety Engineer and the Contractor Safety Engineer (if applicable).

4.5 Problem Log Review, Approval and Closure

Problem log closure requires the instrument Cognizant Engineer's or Project Element Manager's (PEM's) signature.

4.6 PFR Review, Approval and Closure

Each PFR shall be subjected to a review, approval, and closure process as follows:

a. The instrument cognizant engineer and reliability engineer shall perform a preliminary review of each PFR. Each PFR shall be assessed and rated for safety concerns, assigned a cause code, and a cause/corrective action rating.

b. PFRs ready for closure shall be sent to the appropriate signatories prior to a PFR review board meeting.

c. The PFR review board shall meet to review, approve and sign PFRs on a regular basis. Closure of a PFR requires that all appropriate signatures are on the PFR as follows:

(1) Contractor's Instrument Cognizant Engineer and/or Project Element Manager for all PFRs.

(2) Contractor's Instrument Hardware and/or Software Reliability Engineer for all PFRs.

(3) JPL Science Instrument Payload Manager for PFRs which:

(a) Result in an ECR to OP/SP Science Instrument hardware or software

(b) Result in a waiver to level 4 or higher functional requirements

(c) Have an unknown cause

(d) Have a cause/corrective action rating of 3 or 4

In addition, the instrument cognizant engineer or reliability engineer can decide that any other PFR should be reviewed by the JPL Science Instrument Payload Manager.

(4) Contractor's Safety Engineer will review all PFRs to assess for hardware or personnel safety issues.

(5) JPL Mission Assurance Manager for all PFRs with a rating >1/1.

(6) OP/SP Project Manager for Red Flag PFRs.

5. Quality Assurance

5.1 General Requirements

A formal quality assurance or inspection system shall be utilized to provide for documentation and verification of fabrication and assembly processes, functional and performance tests, systems integration and qualification tests.

Quality assurance systems meeting the requirements of ISO 9000 or MIL-Q-9858 and Inspection systems meeting the requirements of MIL-I-45208 or the appropriate subset of ISO 9000 are preferred but not required.

Verification methodologies and acceptance criteria shall be developed in conjunction with the packaging design. Quality Assurance/Inspection Instructions or Procedures shall be generated as needed.

5.2 Implementation Requirements

Hardware procured, fabricated, assembled and tested for OP/SP Science Instruments shall be processed, controlled and documented in accordance with the doing organization's in-place Quality Assurance or Inspection system.

All processes used in the fabrication and assembly of OP/SP Science Instruments shall be documented and qualified prior to use by a flight mission. All workmanship standards and fabrication planning shall be reviewed and approved by JPL Quality Assurance. A list of qualified materials and processes, traceable to the qualification documents, shall be maintained as part of the OP/SP Science Instrument configuration.

All hardware produced for OP/SP Science Instruments shall be fabricated and tested using approved drawings, planning, and procedures, redlined as necessary, and updated at the completion of EM hardware build and test. Redlines shall be formally incorporated into Protoflight or Flight Model (FM) drawings. A redline control procedure, adequate to assure that all changes made during build and test are accurately incorporated into the deliverables documentation, shall be implemented.

Configuration verification of the OP/SP Science Instruments shall be to the functional subassembly level for EM's and to the piece part level for Protoflight and FM's. Material traceability shall be sufficient to accurately identify all materials used in the OP/SP Science Instruments qualification hardware.

Configuration logs shall be maintained for all OP/SP Science Instruments identifying assembly status and configuration. Baseline configurations will be generated for each subsystem and system qualification test.

In-process workmanship inspections of OP/SP Science Instruments shall be performed to verify hardware integrity for environmental tests. Any rework or modification shall be documented. In addition, flight hardware will have workmanship inspections performed at subassembly and assembly levels.

JPL Quality Assurance shall support all project reviews (e.g. design, test readiness, pre-delivery) and certify all deliverables. In particular, a rigorous review of the OP/SP Science Instrument deliverable data shall be performed, in conjunction with the responsible engineering personnel and the project office, to assure that all necessary information, including drawings, fabrication and assembly processes, and test procedures, is adequate to allow the user project to integrate flight hardware and has been included in the data package.

6. Software Assurance

Software developed to execute on hardware embedded in the Science Instrument assembly shall be analyzed for system safety criticality and impact on personnel safety related to the launch vehicle. Software developed to execute on hardware external to the instrument (e.g., system flight computer) shall conform to the software assurance requirements as defined in the Mission Data System (MDS) Software Assurance Standard Requirements (TBD).

7. Materials And Processes

7.1 Selection of Materials and Processes

All materials and processes shall be qualified for the application in which they are used. The contractor's existing preferred materials lists can be used, subject to review and approval by the JPL OP/SP Materials and Processes (M&P) Engineer.

7.2 Submittal of Material Identification and Usage Lists

Material Identification and Usage Lists (MIUL) for packaging and cabling, fasteners, materials, processes, mechanical parts, and special parts shall be submitted by all designers (JPL, subsystem contractors and suppliers). Each MIUL shall contain the information described in the forms. A sample MIUL form can be found in the Outer Planets Program Library, available over the Internet at URL http://outerplanets.LaRC.NASA.gov/outerplanets. These forms will be filled out where applicable and submitted for review and approval by the JPL OP/SP M&P Engineer one month prior to a subsystem Preliminary Design Review (PDR) and subsequently one month prior to the Critical Design Review (CDR). Any open or unresolved issues are to be discussed at the CDR.

7.3 Material Outgassing

Material outgassing limits will be established to meet science instruments and sensor contamination requirements. Only those organic materials with a total mass loss (TML) of less than 1.00 percent and a collected volatile condensable mass (CVCM) of less than 0.10 percent, when tested in accordance with JSC SP-R-0022A "Vacuum Stability Requirements of Polymeric Materials For Spacecraft Applications", or contractor equivalent, are acceptable for general space flight use.

7.4 Hazardous Materials

All materials that are exposed to toxic or hazardous fluids shall be evaluated for compatibility with the fluid in their application. A hazardous fluid is any fluid that could chemically or physically degrade the system. All materials that are exposed to the fluid shall be rated compatible per MSFC-HDBK-527/JCS-09604. Materials rated “A” are acceptable, while those rated “B” shall be batch tested. Existing data showing compatibility may be used if it is approved by OP/SP M&P Engineer.

7.5 Flammable Materials

Materials shall be noncombustible or self-extinguishing to the greatest extent possible and conform with the flammability requirements of NHB 8060.1. Where flammable materials must be used, the standard hazard elimination and control requirements apply as follows: (a) two-failure tolerance on ignition sources, (b) physical separation of the flammable material from ignition sources, and (c) elimination of flame propagation paths.

7.6 Stress Corrosion Cracking

The use of A-rated materials per MSFC-HDBK-527/JSC-09604, or Table I materials per MSFC-SPEC-522, is acceptable. The materials listed in Table III, or "C" rated, should be considered for use only in applications where it can be demonstrated conclusively that the probability of stress corrosion is remote. If Tables II and III, or "C" rated, materials (or materials not listed in MSFC-SPEC-522 or MSFC-HDBK-527/JSC-09604) are planned to be used, their application is subject to approval by JPL OP/SP M&P Engineer.

7.7 Welding

All welding operators of automatic, semi-automatic, or manual welding equipment shall be qualified in accordance with MIL-STD-1595 or a qualification procedure approved by the JPL OP/SP Materials Engineer. Weld rod or wire used as a filler metal on structural parts shall be fully certified and documented for composition, type, heat number, manufacturer, and supplier to provide positive traceability to the end-use item. All fracture-critical welds shall be non-destructively inspected per the requirements of JPL D-5813 "Fracture Control Implementation Plan."

7.8 Non-Destructive Inspection

Non-Destructive Evaluation (NDE) shall be conducted on highly stressed and mission- or safety-critical items. Non-destructive inspection (NDI) techniques shall meet the requirements of MIL-I-6870 (or contractor equivalent) for dye penetrant, magnetic particle, radiographic, eddy current, and ultrasonic inspection.

7.9 Shelf-Life Limited Life Materials

All materials with shelf-life sensitivity, such as polymeric "O" rings and other such seals, shall be used within their life limits.

7.10 Magnetic Materials

The use of magnetic materials shall be limited, as necessary, to meet spacecraft or instrument magnetic requirements.

7.11 Space Environment and Atomic Oxygen Resistance

All materials shall be evaluated for their performance in the anticipated mission environment. Particular attention will be given to the thermal, vacuum, atomic oxygen, UV and electron/proton radiation environment on materials. The JPL OP/SP M&P Engineer will review existing data on materials and recommend environmental test programs where deemed necessary. The JPL OP/SP M&P Engineer will review all plans for environmental testing of materials.

All materials considered for use on the external surface of spacecraft intended for low-earth-orbit operations shall be evaluated for their resistance to atomic oxygen erosion. NASA-TM-100351, "Material Selection Guidelines to Limit Atomic Oxygen Effects on Spacecraft Surfaces" shall be used as a guideline in determining the amount of oxygen incident on materials. Proposed tests to simulate these effects shall be subject to the JPL OP/SP M&P Engineer approval.

7.12 Design Allowables for Structural Parts

Only the statistically based material property allowables contained in MIL-HDBK-5 and the properties contained in MIL-HDBK-17 shall be used for structural analysis. Any other source of material strength or mechanics data (e.g. data sheets, handbooks, etc.) used for structural analysis shall be approved by the JPL OP/SP M&P Engineer.

7.13 Fasteners

Fasteners shall be selected from the JPL Preferred Fastener List (PFL) contained in JPL STD-00009, or contractor equivalent. Exceptions shall be submitted to the JPL Fastener Specialist in the Mechanical Systems Section, for approval. Where fasteners are used in critical applications, document FS 511316 "Detail Specifications for Qualification of Critical Fasteners" shall be followed.

All externally threaded fasteners used for flight applications must be certified. Fasteners used in structural applications must have critical certification. Critical certification requires documentation of chemical and physical test results traceable to both heat and lot numbers. Fasteners used in non-structural applications must have, as a minimum, a certificate of conformance.

7.14 Static Charge Sensitivity

The degree to which differential charging of exposed-to-space materials must be limited depends on the degree of sensitivity to electrostatic discharge (ESD). For those cases in which ESD must be limited to some maximum permissible amount, guidelines identified in the documentation shall be followed. The requirements of JPL D-1348 Rev.A, "JPL Handbook for Electrostatic Discharge Control", or contractor equivalent, shall apply for all other situations.

7.15 Alerts

Materials used in OP/SP flight hardware that are identified in a Government/ Industry Data Exchange Program (GIDEP), NASA Safety, or JPL Quality Alerts shall be evaluated for relevance to the mission environment.

8. Contamination Control

Science Instrument PI's shall submit a Contamination Control Plan to the JPL OP/SP Mission Assurance Manager for review. The Plan shall indicate how Contamination Control will mitigate against instrument degradation and how cleanliness will be maintained during shipping and integration to the spacecraft. All pyrotechnic devices shall use a NASA Standard Initiator.

9. Configuration Management

Science Instrument PI's shall submit a Configuration Control Plan to the JPL Mission Assurance Manager for review. The Plan shall address which items are to be controlled and to what level and address the process for Configuration Control.

10. Safety Requirements

Safety on the Outer Planets/Solar Probe Project is separated into three distinct areas:

1) Demonstration of compliance with Federal Occupational Safety and Health Administration (Fed-OSHA) requirements; and
2) demonstration of appropriate safety plans and procedures for protection of the flight hardware; and
3) support of the spacecraft level safety review process for approval to launch on the Space Transportation System (STS).

In support of item 1), a copy of the PI organization's Institutional Health and Safety Plan per procurement instructions will be required.

In support of item 2), an existng generic safety plan, or one developed specifically for this Instrument, which describes processes the PI employs to ensure protection of the flight hardware, will be required. These processes should include basic flight hardware security, hardware handling practices, personnel training requirements, and pretest/pre-transportation readiness reviews or assessments.

In support of item 3), descriptive information and diagrams detailing the design and operation of each Instrument will be required. The extent of the details will depend on the hazards involved. As a minimum, detailed structural and material analyses will be required. Descriptions of verification methods and process will be required for each hazard.

The overall Systems Safety process will be tailored as necessary for each specific instrument, yet provide assurance to Program and STS management that the safety of the hardware and proper control of hazards has been implemented.